Book of Knowledge

Maurice Schippers

A book with numbers coming out of it

Description automatically generated

Author: Maurice Schippers

Class: RB02-Eindhoven

Course: ICS-CS4

Date published: t.b.d.

Version: 1.0

Table of Contents:

[1 Introduction and Personal BoK Approach 3](#_Toc145343137)

[1.1 Basic Hacking and Pentesting Process 3](#_Toc145343138)

[1.2 Threat + Risk Analysis and CIA 3](#_Toc145343139)

[2 Web: Application Attack and Defense 4](#_Toc145343140)

[2.1 Footprinting, Reconnaissance and Social Engineering 4](#_Toc145343141)

[2.2 Path Traversal, (remote) File inclusion and Command Injection 4](#_Toc145343142)

[3 Web: Database Attack and Defense 5](#_Toc145343143)

[3.1 Web Application Firewalls 5](#_Toc145343144)

[3.2 SQL Injection 5](#_Toc145343145)

[4 Web: Site Attack and Defense 6](#_Toc145343146)

[4.1 Host Intrusion Detection and Prevention (HIDS) 6](#_Toc145343147)

[4.2 XSS & CSRF 6](#_Toc145343148)

[5 Network: Identification of Vulnerabilities 7](#_Toc145343149)

[5.1 Network Scanning and Enumeration (incl. Sniffing) 7](#_Toc145343150)

[5.1.1 How to securely host a Web Shop with Secure Network Connections (HTTPS/TLS/SSH) 7](#_Toc145343151)

[5.2 Law & Ethics and Responsible Disclosure + GDPR 7](#_Toc145343152)

[6 Network: Protect the Network 8](#_Toc145343153)

[6.1 Network Separation and Segmentation 8](#_Toc145343154)

[6.2 VPN: How to manage a Web Shop with Secure Remote Access 8](#_Toc145343155)

[7 Network: Attack the Network 9](#_Toc145343156)

[7.1 Network Spoofing and Man in The Middle Attacks (MITM) 9](#_Toc145343157)

[7.2 WiFi Hacking 9](#_Toc145343158)

[8 Network: Monitor and Detect 10](#_Toc145343159)

[8.1 Network Intrusion Detection and Prevention (NIDS/IPS) 10](#_Toc145343160)

[8.2 IT Monitoring 10](#_Toc145343161)

[8.2.1 IT Basic Monitoring (Availability) 10](#_Toc145343162)

[8.2.2 IT Security Monitoring (Confidentiality and Integrity) 10](#_Toc145343163)

[9 Concepts: Identity Management, Authentication and Access Control 11](#_Toc145343164)

[9.1 Identity Management, Authentication and Access Control 11](#_Toc145343165)

[9.2 Password Cracking (system and network) 11](#_Toc145343166)

[10 Concepts: Incident Response and Analysis 12](#_Toc145343167)

[10.1 Security Incident Management 12](#_Toc145343168)

[10.2 IT System Hardening + Common Vulnerabilities and Exposures (CVE's) 12](#_Toc145343169)

[11 Overall Conclusion 13](#_Toc145343170)

[12 References 14](#_Toc145343171)

# Introduction and Personal BoK Approach

Welcome to my personal Book of Knowledge (BoK) document. My name is Maurice Schippers, and I am a student in the Cyber Security specialization course. I have always had a passion for this subject ever since I started my career in ICT. I think security is one of the most important aspects of IT considering how many people use computers of any type nowadays and the vulnerability of the data that is stored everywhere. With the rise of AI on the horizon, it will become more challenging to defend, and it has proven to be much easier for black-hat hackers to create malware tools (Sabin, 2023).

This document serves as a reflection of my learning progress through the different subjects. For each of the subjects, I will be gathering information from different sources, starting with Canvas, and branch out from there when needed. I also aim to get some hands-on experience for each of the subjects. After all: “*Theory will take you only so far*”.

## Basic Hacking and Pentesting Process

* What are the process steps of every pentest in general?
* What are the minimal requirements for a good pentest contract and pentest report?

## Threat + Risk Analysis and CIA

x

# Web: Application Attack and Defense

## Footprinting, Reconnaissance and Social Engineering

x

## Path Traversal, (remote) File inclusion and Command Injection

x

# Web: Database Attack and Defense

## Web Application Firewalls

x

## SQL Injection

x

# Web: Site Attack and Defense

## Host Intrusion Detection and Prevention (HIDS)

x

## XSS & CSRF

x

# Network: Identification of Vulnerabilities

## Network Scanning and Enumeration (incl. Sniffing)

x

### How to securely host a Web Shop with Secure Network Connections (HTTPS/TLS/SSH)

x

## Law & Ethics and Responsible Disclosure + GDPR

x

# Network: Protect the Network

## Network Separation and Segmentation

x

## VPN: How to manage a Web Shop with Secure Remote Access

x

# Network: Attack the Network

## Network Spoofing and Man in The Middle Attacks (MITM)

x

## WiFi Hacking

x

# Network: Monitor and Detect

## Network Intrusion Detection and Prevention (NIDS/IPS)

x

## IT Monitoring

Split on CIA:

### IT Basic Monitoring (Availability)

x

### IT Security Monitoring (Confidentiality and Integrity)

x

# Concepts: Identity Management, Authentication and Access Control

## Identity Management, Authentication and Access Control

x

## Password Cracking (system and network)

x

# Concepts: Incident Response and Analysis

## Security Incident Management

x

## IT System Hardening + Common Vulnerabilities and Exposures (CVE's)

x

# Overall Conclusion

# References

Sabin, S. (2023, January 10). *Hackers are already abusing ChatGPT to write malware*. Axios. Retrieved September 11, 2023, from https://www.axios.com/2023/01/10/hackers-chatgpt-malware-cybercrime-ai